(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 April 2005 (14.04.2005)

PCT

(10) International Publication Number
WO 2005/034514 A1

(51) International Patent Classification[7]: H04N 7/167, H04L 9/30

(21) International Application Number: PCT/EP2004/052445

(22) International Filing Date: 5 October 2004 (05.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03292459.9 6 October 2003 (06.10.2003) EP

(71) Applicant *(for all designated States except US)*: **Canal+ Technologies** [FR/FR]; 34, place Raoul Dautry, F-75906 Paris (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GUILLOT, Philippe** [FR/FR]; c/o Canal+ Technologies, 34, place Raoul Dautry, F-75906 Paris (FR). **ALBANESE, Laurent** [FR/FR]; c/o Canal+ Technologies, 34, place Raoul Dautry, F-75906 Paris (FR).

(74) Agent: **WEIHS, Bruno**; Osha & May, 121, avenue des Champs Elysées, F-75008 Paris (FR).

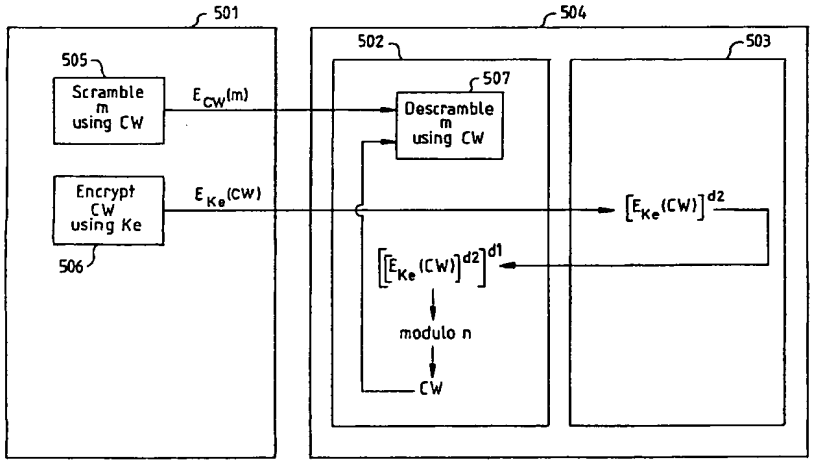
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: PORTABLE SECURITY MODULE PAIRING



(57) Abstract: A method for pairing a first element and a second element, wherein the first element and the second element form a first decoding system among a plurality of receiving decoding systems in a broadcasting network. Each receiving decoding system is adapted to descramble scrambled audiovisual information received over the broadcasting network. A first key unique in the broadcasting network is selected. A second key is determined according to the first key, such that a combination of the first key and the second key enables to decrypt broadcasted encrypted control data that is received to be decrypted by each receiving decoding system, the encryp ted control data being identical for each receiving decoding system. The first key and the second key are assigned respectively to the first element and the second element.

WO 2005/034514 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.